Waterton
Academy Trust

Counter Fraud, Irregularity and Cybercrime Policy

watertonacademytrust.org

Contents

Introduction

The Trust is responsible for the stewardship of public funds and charitable assets. It must ensure that resources are used only for the purposes intended, in accordance with the Trust's funding agreement, charitable objects, legal duties and the Academy Trust Handbook.

The board of trustees is responsible for maintaining effective governance, risk management, internal control and assurance arrangements to prevent, detect and respond to fraud, theft, irregularity, cybercrime and related wrongdoing.

This policy supports the Trust's compliance with the Academy Trust Handbook 2025. It reflects the requirement for academy trusts to be aware of fraud, theft and irregularity risks, put proportionate controls in place, take appropriate action where suspected or identified, and notify DfE where required.

This policy also reflects DfE guidance on fraud awareness and reporting in education, DfE good practice on internal scrutiny, and the fraud-prevention principles set out in guidance on the offence of failure to prevent fraud under the Economic Crime and Corporate Transparency Act 2023.

This policy should be read alongside the Trust's Financial Management Policy, Procurement Policy, Reserves Policy, Investment Policy, Whistleblowing Policy, Code of Conduct for Employees Policy, Gifts and Hospitality Policy, Data Protection Policy, Disciplinary Policy and Internal Scrutiny arrangements.

Policy Statement

The Trust has a zero-tolerance approach to fraud, theft, bribery, corruption, money laundering, deliberate financial irregularity, cybercrime and conduct that exposes the Trust to failure to prevent fraud risk.

The Trust will maintain a counter-fraud culture in which honesty, openness, accountability, regularity, propriety and value for money are expected at all levels.

The Trust will maintain proportionate preventative and detective controls. These include segregation of duties, documented procedures, approval limits, reconciliations, audit trails, cyber controls, due diligence, declarations of interest, training, reporting routes and independent assurance.

All trustees, local governors, senior leaders, budget holders and managers must set an example by complying with this policy and the Trust's control framework. They must not override controls except through properly authorised and documented arrangements.

The Trust will investigate concerns promptly and objectively, protect whistleblowers, preserve evidence, take disciplinary, civil, criminal or regulatory action where appropriate, seek recovery of losses, and learn lessons to strengthen controls.

Aims

The aims of this policy are to:

- Promote a culture of honesty, openness, accountability and stewardship of public funds.
- Prevent, detect and respond to fraud, theft, irregularity, bribery, corruption, money laundering, cybercrime and related wrongdoing.
- Provide clear reporting routes for staff, trustees, local governors, suppliers and others working with the Trust;
- Ensure concerns are investigated fairly, confidentially and proportionately;
- Support compliance with the Academy Trust Handbook, DfE guidance and relevant legislation; and
- Ensure lessons are learned and controls are strengthened following any incident.

Definitions

Fraud

Fraud includes false representation, failing to disclose information where there is a legal duty to do so, or abuse of position, where the conduct is dishonest and intended to make a gain, cause loss, or expose another to a risk of loss

Theft

Theft is the dishonest appropriation of property belonging to another with the intention of permanently depriving the other of it.

Irregularity

Irregularity means non-compliance with legislation, the funding agreement, the Academy Trust Handbook, delegated authorities, policies, financial procedures, procurement rules or other requirements relating to public funds.

Bribery and Corruption

Bribery includes offering, promising, giving, requesting, agreeing to receive or accepting a financial or other advantage to induce improper performance. Corruption includes abuse of entrusted power for private gain.

Money Laundering

Money laundering is the process by which criminal property is concealed, converted, transferred or made to appear legitimate.

Cybercrime and cyber-enabled fraud

Cybercrime includes unauthorised access, ransomware, malware, phishing, business email compromise, data theft, denial of service, and manipulation of finance, payroll, HR or pupil systems. Cyber-enabled fraud includes fraud carried out through digital systems or communications.

Associated person

For failure to prevent fraud purposes, an associated person may include an employee, agent, subsidiary undertaking or other person providing services for or on behalf of the Trust, depending on all relevant circumstances.

Scope

This policy applies to the whole Trust, including all academies, central services and any subsidiary or connected entity controlled by the Trust.

It applies to members, trustees, local governors, the Accounting Officer, the Chief Financial Officer, senior leaders, employees, agency workers, volunteers, contractors, suppliers, consultants, service providers, partners and others working for or on behalf of the Trust.

Where the Trust contracts with third parties, it will take a proportionate risk-based approach to ensuring that contractual terms, due diligence and monitoring arrangements support the Trust's counter-fraud expectations.

Failure by an employee to comply with this policy may lead to disciplinary action, up to and including dismissal. Failure by a supplier, contractor, consultant or other third party may lead to termination of contract, recovery action, exclusion from future procurement and/or referral to law enforcement or regulators.

Failure to Prevent Fraud Requirements

The Trust will maintain arrangements designed to prevent fraud by persons associated with the Trust and to demonstrate reasonable fraud prevention procedures where the Trust is in scope of the offence of failure to prevent fraud under the Economic Crime and Corporate Transparency Act 2023.

The offence applies to large organisations. For the purposes of the Failure to Prevent Fraud offence, the Trust will assess whether it meets two or more of the statutory large-organisation criteria: more than 250 employees, more than £36 million turnover, and more than £18 million in total assets. The assessment will be undertaken annually and following any material structural, financial or organisational change. Where the Trust is uncertain whether it is in scope, it will obtain appropriate professional or legal advice.

Whether or not the Trust is legally in scope at a particular time, the Trust will adopt the failure to prevent fraud principles as good practice because they support stewardship of public funds and align with the Academy Trust Handbook requirement for proportionate controls.

The Trust's approach is based on six fraud-prevention principles: top-level commitment; fraud risk assessment; proportionate risk-based prevention

procedures; due diligence; communication and training; and monitoring and review.

The Trust will not seek to benefit from fraud, even where rejecting an opportunity may result in delay, additional cost, lost income or reputational challenge. Staff and associated persons must not make false, misleading or incomplete statements or records to secure funding, contracts, performance benefits or other advantage for the Trust.

Failure to prevent fraud risks will be considered in relation to staff, agency workers, contractors, consultants, subsidiary undertakings, outsourced service providers, payroll, recruitment, procurement, estates, lettings, grant claims, pupil census, free school meals, high needs funding, bursaries and other funding returns.

The Chief Financial Officer will maintain a failure to prevent fraud assessment, supported by the Governance Professional, relevant senior leaders and, where appropriate, legal advisers.

The assessment will be reported to the Audit and Risk Committee at least annually.

Fraud Prevention Framework

The Trust will maintain a documented fraud-prevention framework. The framework links governance expectations, risk assessment, controls, due diligence, reporting, assurance and continuous improvement.

Principle	Trust approach	Evidence / assurance
Top-level commitment	Board, Accounting Officer, CFO and senior leaders promote an anti-fraud culture, reject fraudulent gain and ensure resources are available for prevention and detection.	Board minutes, policy approval, training records, leadership communications, committee reports.
Risk assessment	Fraud risks are identified, assessed and reviewed across all academies and central functions, including failure to prevent fraud and cyber-enabled fraud risks.	Fraud risk assessment, risk register, incident logs, audit findings, DfE alerts.
Proportionate procedures	Controls are proportionate to risk and include procedures, approval limits, segregation of duties, reconciliations, exception reporting and cyber controls.	Financial regulations, scheme of delegation, process notes, reconciliations, access reviews, control testing.
Due diligence	Risk-based checks are undertaken for employees, trustees, local governors, suppliers, contractors, agents, consultants and related parties.	Recruitment checks, declarations of interest, supplier due diligence, procurement records, related party evidence.
Communication and training	Staff and relevant third parties understand reporting routes, fraud indicators, expected behaviours and consequences of breach.	Induction records, annual declarations, fraud alerts, training completion, supplier communications.

Monitoring and review	Controls are reviewed through management checks, internal scrutiny, external audit, fraud logs, incident reviews and Audit and Risk Committee oversight.	Internal scrutiny reports, external audit management letters, action trackers, committee minutes, annual review.

The framework will be reviewed at least annually, following any significant incident, DfE investigation, audit finding, cyber incident, organisational change or change in legislation or guidance.

Fraud Risk Assessment Approach

The Trust will maintain a fraud risk assessment that identifies inherent risks, existing controls, residual risk, control owners, further actions, target dates and assurance sources.

Fraud risks will be reviewed at least annually through the Trust's existing risk management, internal scrutiny and Audit and Risk Committee reporting cycle. A more detailed fraud risk assessment will be undertaken where required, including for high-risk areas, significant incidents or attempted fraud, cyber incidents, DfE alerts, new or changed funding streams, material changes in systems or controls, academy growth, or changes in the external threat environment.

The assessment will consider financial and non-financial fraud risks, including management override, cultural risk, pressure to meet targets, weaknesses in segregation of duties, capability gaps, staff turnover and cyber-enabled fraud.

The assessment will be informed by the Trust's risk register, internal scrutiny findings, external audit findings, DfE fraud alerts, DfE investigation reports, whistleblowing reports, fraud logs, cyber incident reports and management information.

The Chief Financial Officer will coordinate the assessment with input from central finance, HR, IT, estates, procurement, governance, academy leaders and budget holders. The Audit and Risk Committee will review the assessment and challenge whether controls and assurances are sufficient.

High or increasing fraud risks will be escalated to the risk register and considered when setting the internal scrutiny programme and training plan.

Assurance Arrangements and Internal Scrutiny

The Trust will maintain sound internal control, risk management and assurance processes. Assurance will follow a tiered approach: clearly communicated procedures, structures and staff training; day-to-day supervision and management checks; internal scrutiny overseen by the Audit and Risk Committee; and external audit and assurance.

The Trust must have a programme of internal scrutiny to provide independent assurance to the board that financial and non-financial controls and risk management procedures are operating effectively.

Internal scrutiny will be risk-based and informed by the risk register, fraud risk assessment, previous incidents, changes in systems, DfE alerts, DfE reviews, external audit findings and Audit and Risk Committee priorities.

Internal scrutiny may include reviews of anti-fraud arrangements, procurement, payroll, expenses, pupil census, free school meals, high needs funding, school funds, lettings income, cyber security, gifts and hospitality, related party transactions and declarations of interest.

Internal scrutiny findings, fraud risk assessment outcomes and action progress will be reported to the Audit and Risk Committee. The annual internal scrutiny summary report will be made available to all trustees promptly and submitted to DfE by 31 December each year, alongside the audited annual accounts. The Trust will also provide DfE with any other internal scrutiny reports if requested.

Management will maintain an action tracker for internal scrutiny, external audit, DfE review, RPA risk management audit, cyber security and fraud investigation recommendations. The Audit and Risk Committee will monitor timely completion and challenge overdue or ineffective actions.

Declarations of Interest, Gifts and Hospitality

The Trust will maintain an up-to-date register of relevant business and financial interests for members, trustees, local governors and senior employees, and any other roles required by the Trust's policy or the Academy Trust Handbook.

The register will include relevant interests arising from close family relationships between members, trustees, local governors and employees, and between those individuals and employees, in accordance with the Academy Trust Handbook.

Declarations must be completed on appointment, reviewed at least annually and updated promptly when circumstances change. Nil returns must be recorded where applicable.

Individuals must declare actual, potential or perceived conflicts of interest at the start of meetings and before taking part in decisions, procurement, recruitment, contract management, related party transactions, appointments, disposals or other matters where an interest could arise.

The Trust will publish the register of business and financial interests for members, trustees, local governors and the Accounting Officer as required by the Academy Trust Handbook, subject to permitted discretion and safeguarding of personal information.

Gifts and hospitality must be declared and managed in accordance with the Trust's Gifts and Hospitality Policy. Gifts, hospitality, donations or sponsorship must not influence, or appear to influence, decision-making. Suspected inducements, bribery or attempts to influence decisions must be reported under this policy.

Breaches of declaration requirements, failure to withdraw from conflicted decision-making, undisclosed related party transactions or acceptance of improper gifts may constitute irregularity, misconduct, bribery or fraud and will be investigated accordingly.

Roles and Responsibilities

Board of Trustees

The board has ultimate responsibility for governance, risk management, internal control, assurance, stewardship of public funds and compliance with the Academy Trust Handbook. It must approve this policy, maintain oversight of fraud risks, ensure DfE notification where required and retain ultimate oversight of the risk register, drawing on advice from the Audit and Risk Committee.

Audit and Risk Committee

The Audit and Risk Committee oversees internal scrutiny, risk management, fraud prevention, whistleblowing, external audit findings and this policy. It must oversee and approve the internal scrutiny programme, ensure risks are addressed appropriately, report to the board on the adequacy of internal controls and risk management, review fraud and irregularity reports, monitor action trackers and ensure appropriate follow-up.

Accounting Officer / Chief Executive Officer

The Accounting Officer is responsible for a culture of regularity, propriety, value for money and accountability, and for ensuring that suspected fraud, theft, irregularity and cybercrime are addressed promptly and escalated where appropriate.

Chief Financial Officer

The CFO is the lead senior officer for counter-fraud coordination, maintenance of the fraud and irregularity register, financial control, DfE notification preparation, fraud risk assessment, failure to prevent fraud assessment and reporting to the Accounting Officer and Audit and Risk Committee.

Governance Professional

The Governance Professional supports reporting to the board and committees, maintains governance records, supports declaration of interest processes and provides an alternative reporting route where concerns involve senior leaders.

Executive Headteachers, Headteachers, Leaders and Budget Holders

Leaders and budget holders must maintain effective controls, ensure staff comply with procedures, review risks, complete declarations, report concerns promptly,

protect evidence and implement actions arising from audits, investigations and risk assessments.

Staff and other persons within scope

Everyone covered by this policy must act honestly, comply with policies and procedures, protect Trust assets and information, complete required declarations, avoid conflicts of interest and report actual or suspected fraud, theft, irregularity, bribery, corruption, money laundering or cybercrime without delay.

Examples of Fraud, Theft, Irregularity and Cybercrime

The following examples are not exhaustive. Concerns should be reported even where there is uncertainty about whether the conduct meets a formal legal definition.

- False or inflated invoices, duplicate invoices, payment diversion or mandate fraud.
- Procurement fraud, bid rigging, collusion, conflicts of interest or failure to follow tendering requirements.
- Misuse of purchasing cards, school funds, petty cash, lettings income, trips income or charitable funds.
- Payroll fraud, false overtime or expenses claims, ghost employees, pension irregularities or unauthorised payments.
- False pupil census, free school meal, high needs, bursary, grant or other funding claims.
- Falsification of records, including registers, timesheets, recruitment documents, qualifications, references, financial records or management information.
- Theft or unauthorised use of cash, equipment, stock, data, devices, vehicles, facilities or intellectual property.
- Abuse of position, including favouritism, improper related party transactions or using Trust assets for private benefit.
- Bribery, facilitation payments, improper gifts, hospitality or inducements.
- Phishing, ransomware, malware, unauthorised access, compromised accounts, data exfiltration or manipulation of finance, payroll or pupil systems.
- Attempting to conceal losses, control weaknesses, breaches of delegated authority or non-compliance with the Academy Trust Handbook.
- Conduct by a person associated with the Trust that dishonestly seeks to benefit the Trust, such as false reporting to obtain funding or misleading procurement or performance information.

Prevention and Control Environment

The Trust will maintain proportionate controls to reduce the risk of fraud, theft, irregularity and cybercrime. These include, but are not limited to:

- Clear governance arrangements, terms of reference and delegated authorities.
- Monthly management accounts and regular budget monitoring.
- Segregation of duties for ordering, approving, receiving goods or services, invoice processing, payment approval and bank administration.
- Procurement controls, supplier due diligence, contract management and value for money checks.
- Complete, accurate and up-to-date records, reconciliations and audit trails.
- Secure banking arrangements, dual authorisation and independent verification of changes to supplier or employee bank details.
- Asset registers, stock checks, physical security controls and secure disposal processes.
- Registers of business and financial interests, gifts and hospitality declarations and related party transaction controls.
- Appropriate recruitment checks, induction, staff code of conduct and mandatory training.
- Cyber security controls, including multi-factor authentication where appropriate, secure password practices, phishing awareness, backup arrangements, patching, privileged access controls and incident response arrangements.
- Fraud risk assessment, internal scrutiny, external audit and Audit and Risk Committee oversight.
- Business continuity, insurance or RPA arrangements and lessons learned after incidents.

Reporting Concerns

Any actual or suspected fraud, theft, irregularity, bribery, corruption, money laundering, cybercrime or failure to prevent fraud risk must be reported without delay. Reports may be made to the line manager, Headteacher, Chief Financial Officer, Accounting Officer, Governance Professional, Chair of the Audit and Risk Committee or through the Whistleblowing Policy.

Where the concern involves the Chief Financial Officer, it should be reported to the Accounting Officer and Chair of the Audit and Risk Committee. Where it involves the Accounting Officer, it should be reported to the Chair of Trustees and Chair of the Audit and Risk Committee. Where it involves the Chair of Trustees, it should be reported to the Members and/or DfE as appropriate.

Individuals should not investigate concerns themselves, confront suspected individuals, remove evidence without authority, alert suspected individuals, or discuss allegations with anyone who does not have a legitimate need to know.

The Trust will maintain a confidential fraud, theft, irregularity and cybercrime register. The register will record concerns raised, action taken, referrals, losses, recoveries, control weaknesses, lessons learned and reporting to DfE or other bodies.

DfE, Police, Auditor and Other External Reporting

In line with the Academy Trust Handbook 2025, the board of trustees must notify DfE as soon as possible of all instances of fraud, theft or irregularity exceeding £5,000 individually, or £5,000 cumulatively in any financial year. Unusual or systematic fraud, regardless of value, must also be reported.

DfE notification will include full details of the events with dates, the financial value of the loss, measures taken to prevent recurrence, whether the matter was referred to the police and, if not, why, and whether insurance or the Risk Protection Arrangement has offset any loss.

The Trust will also consider DfE reporting where there is suspected fraud or financial irregularity involving DfE funding, breach of funding rules, non-delivery of funded education or training, or other concerns covered by DfE reporting guidance.

The Trust will consider referral to the police, Action Fraud, the National Cyber Security Centre, insurers, the Risk Protection Arrangement, external auditors, internal scrutiny provider, local authority, Charity Commission or other relevant body as appropriate.

External auditors and internal scrutiny providers must be informed of investigation outcomes and matters of fraud, irregularity or impropriety where this may affect audit, assurance, regularity or the annual accounts.

DfE may conduct or commission investigations into actual or potential fraud, theft or irregularity. The Trust will cooperate fully with DfE and its appointed investigators.

Fraud Response Plan

The purpose of the response plan is to define authority levels, responsibilities for action and reporting lines when fraud, theft, irregularity or cybercrime is suspected or identified.

The response plan is designed to protect individuals, pupils, public funds, charitable assets, data, systems and the reputation of the Trust; prevent further loss; establish and secure evidence; assign investigation responsibility; notify DfE and other external bodies; quantify and recover losses; take proportionate action; and strengthen controls to prevent recurrence.

The Chief Financial Officer and Accounting Officer will normally determine the initial response, in consultation with the Chair of the Audit and Risk Committee and HR, legal, IT, internal scrutiny or external audit advisers where appropriate.

Where there is a requirement to notify DfE, the Trust will make notification as soon as possible and will consider whether to pause or scope any investigation to avoid prejudicing DfE, police or other external action.

Investigation Procedures and Evidence

The Trust will appoint an appropriate investigator, which may be a senior leader, internal scrutiny provider, external auditor, HR adviser, legal adviser, cyber specialist or other independent specialist depending on the nature of the concern.

Investigations must be proportionate, objective, timely and documented. Investigators must consider whether specialist advice is required before accessing, copying, moving or analysing evidence.

Evidence must be preserved securely. This may include documents, emails, system logs, CCTV, access records, bank records, supplier records, personnel files, declarations of interest, procurement records and device images.

Formal interviews should be conducted in an appropriate setting, normally by at least two people. Notes should be taken and agreed where possible. Employees may be accompanied in accordance with HR procedures.

The Trust will follow its Disciplinary Policy, grievance procedures, whistleblowing arrangements, data protection procedures and legal obligations throughout any investigation.

Preventing Further Loss and System Access Controls

Where there are reasonable grounds to suspect an individual or third party of fraud, theft, irregularity or cybercrime, the Trust will consider immediate steps to prevent further loss or damage, including:

- Suspension or temporary change of duties in accordance with HR procedures.
- Withdrawal or restriction of access to finance, payroll, banking, HR, pupil, premises, email and IT systems.
- Recovery of Trust property, identity cards, keys, devices, purchasing cards and security tokens.
- Freezing or review of supplier accounts, purchase orders, contracts or payment runs.
- Independent verification of bank mandate changes and urgent review of recent transactions.
- Preservation of digital evidence, logs and backups.
- Notification to banks, insurers, RPA, police, Action Fraud, NCSC or other relevant bodies where appropriate.

Cyber incidents must be managed in line with the Trust's cyber incident response and business continuity procedures. The Trust must not pay cyber ransom demands.

Confidentiality, Whistleblowing and Data Protection

All concerns and investigations will be handled confidentially and information will be shared only with those who have a legitimate need to know.

The Trust will protect whistleblowers in line with its Whistleblowing Policy and applicable legislation. Staff should be aware of internal reporting routes and external reporting routes, including DfE where appropriate.

Personal data will be processed in accordance with UK GDPR, the Data Protection Act 2018 and the Trust's Data Protection Policy. Where a personal data breach is suspected, the Data Protection Officer will be informed promptly.

Recovery of Losses and Sanctions

Recovering losses is a key objective of any investigation. The Trust will quantify losses and consider reasonable and proportionate recovery action, including repayment, insurance or RPA claims, civil proceedings, contract remedies or criminal compensation.

Where the loss is substantial or there is a risk of dissipation of assets, the Trust will consider obtaining legal advice on preservation or recovery action.

Proven wrongdoing may result in disciplinary action, dismissal, referral to professional bodies, termination of contracts, civil proceedings, referral to law enforcement, DfE notification and/or regulatory reporting.

Requests for references for employees disciplined, dismissed or prosecuted for fraud or related misconduct will be handled by HR in accordance with legal requirements and the Trust's reference policy.

Training and Awareness

The Trust will promote an anti-fraud culture through induction, training, communications, leadership expectations and clear reporting routes.
Staff in higher-risk roles, including finance, payroll, HR, procurement, estates, IT, admissions, census, trip administration and budget management, will receive targeted training or briefings appropriate to their responsibilities.

Training and awareness will include fraud indicators, cyber-enabled fraud, phishing, mandate fraud, conflicts of interest, gifts and hospitality, whistleblowing, DfE reporting expectations and the Trust's failure to prevent fraud approach.

The Trust will consider DfE fraud alerts, published investigation reports and lessons learned from the sector when developing training and communications.

Monitoring, Reporting and Review

The Chief Financial Officer will report to each meeting of the Audit and Risk Committee on the fraud, theft, irregularity and cybercrime register, including nil returns where appropriate.

On completion of any investigation, a written report will normally be submitted to the Audit and Risk Committee, internal scrutiny provider and external auditor, subject to confidentiality and legal constraints. The report should describe the incident, loss value, people involved, method, action taken, control weaknesses, lessons learned and recommendations.

The Audit and Risk Committee will monitor completion of actions arising from investigations, audits, DfE reviews, RPA risk management audits, cyber incidents, fraud risk assessments and failure to prevent fraud assessments.

This policy will be reviewed at least every three years, or sooner if required by the Academy Trust Handbook, DfE guidance, legislation, audit findings, incidents or changes in the Trust's operating model.

Appendix A – Fraud, Theft, Irregularity and Cybercrime Response Checklist

1. Record the concern on the confidential fraud, theft, irregularity and cybercrime register.
2. Assess immediate safeguarding, welfare, data protection, cyber, financial and reputational risks.
3. Notify the Accounting Officer, Chief Financial Officer and Chair of Audit and Risk Committee unless implicated.
4. Secure evidence and restrict access where necessary.
5. Decide investigation route and appoint an independent investigator or specialist.
6. Assess whether DfE, police, Action Fraud, NCSC, insurer/RPA, external auditor or other bodies must be notified.
7. Quantify actual or potential loss and consider recovery options.
8. Maintain confidentiality and protect whistleblowers.
9. Report outcomes and lessons learned to the Audit and Risk Committee and board as appropriate.
10. Update controls, training, risk assessment, risk register and internal scrutiny programme.

Appendix B – Fraud Risk Assessment Methodology and Prompts Sheet

The Trust should use the following methodology when updating its fraud risk assessment:

1. Identify fraud scenarios and associated persons who could create risk.
2. Assess inherent likelihood and impact before controls.
3. Identify preventative, detective and corrective controls.
4. Assess residual likelihood and impact after controls.
5. Record control owners, evidence sources, assurance sources and gaps.
6. Agree further actions with target dates and accountable owners.
7. Escalate high or increasing residual risks to the risk register.
8. Use the assessment to inform internal scrutiny, training and policy review.

Risk areas to consider include:

- Governance: conflicts of interest, related parties, gifts and hospitality, decision-making records and compliance with delegated authorities.
- Funding and returns: pupil census, free school meals, high needs, grants, bursaries and other DfE or local authority returns.
- Income: lettings, trips, catering, uniform, donations, sponsorship, school funds, cash handling and online payments.
- Expenditure: procurement, tendering, purchase orders, contract management, duplicate invoices, supplier due diligence and payment approval.
- Payroll and HR: recruitment checks, ghost employees, changes to pay, overtime, expenses, absence records and pension data.
- Banking and treasury: bank mandate changes, online banking permissions, investments, reconciliations and cash flow controls.
- Assets and estates: equipment, stock, vehicles, leases, disposals, capital projects, insurance claims and facilities access.
- IT and cyber: phishing, ransomware, compromised accounts, privileged access, backups, patching, third-party systems, incident response and cyber awareness.
- Data and records: unauthorised data access, alteration or destruction of records, retention, secure disposal and audit trails.
- Culture and capability: training, management override, pressure to meet targets, staff turnover, segregation of duties and whistleblowing confidence.

Appendix C – Fraud-Prevention Framework Checklist

Area	Question	Evidence / action
Top-level commitment	Has the board approved the counter-fraud policy, communicated zero tolerance and received regular reports?	[Record evidence or action]

Risk assessment	Is there a documented fraud risk assessment covering academy-specific and failure to prevent fraud risks?	[Record evidence or action]
Proportionate procedures	Are controls documented, risk-based, tested and understood by staff?	[Record evidence or action]
Due diligence	Are staff, trustees, governors, suppliers, contractors, agents, related parties and high-risk transactions subject to proportionate checks?	[Record evidence or action]
Communication and training	Do relevant people know the risks, expectations, reporting routes and consequences of breach?	[Record evidence or action]
Monitoring and review	Are management checks, internal scrutiny, external audit and committee oversight providing evidence that controls operate effectively?	[Record evidence or action]

Appendix D – Failure to Prevent Fraud Supplementary Assessment

This appendix does not replace the Trust's fraud-prevention framework checklist at Appendix C. It should be used as a supplementary assessment focused only on Failure to Prevent Fraud exposure and the adequacy of reasonable fraud-prevention procedures.

Area	Question	Evidence / action
Applicability	Has the Trust assessed whether it meets the statutory size criteria for the Failure to Prevent Fraud offence?	[Record evidence or action]
Associated persons	Has the Trust identified who may be an "associated person", including employees, agents, contractors, consultants, outsourced providers and others providing services for or on behalf of the Trust?	[Record evidence or action]
Risk exposure	Could any associated person commit fraud intending to benefit the Trust or a recipient of Trust services, including in funding, pupil data, procurement, HR, payroll, financial reporting, grant claims or contract management?	[Record evidence or action]
Proportionate controls	Are existing controls in Appendix C sufficient to prevent or detect those risks, and are any enhanced controls needed for higher-risk areas?	[Record evidence or action]
Due diligence and contracts	Are higher-risk suppliers, agents, consultants, contractors and outsourced providers subject to appropriate due diligence, contract terms, right-to-audit	[Record evidence or action]

	clauses, termination rights and reporting obligations?	
Communication and training	Have relevant staff and associated persons been informed of the Trust's zero-tolerance approach, reporting routes, and the consequences of fraud?	[Record evidence or action]
Monitoring and assurance	Has the Trust tested the effectiveness of key fraud-prevention measures through management checks, internal scrutiny, external audit, or Audit and Risk Committee review?	
Legal advice and rationale	Has the Trust documented any decision that procedures are not required or are not proportionate, and sought legal advice where scope, liability or reporting duties are uncertain?	

Appendix E – DfE Notification Checklist

Use this checklist when considering whether a matter must be notified to DfE under the Academy Trust Handbook 2025 or DfE reporting guidance.

- Does the matter involve fraud, theft or irregularity exceeding £5,000 individually?
- Does the matter cause cumulative fraud, theft or irregularity losses exceeding £5,000 in the financial year?
- Is the matter unusual or systematic, regardless of value?
- Does the matter involve suspected or proven deception in DfE funding, funding rules or delivery of funded education or training?
- Have full details, dates, financial loss, recurrence prevention, police referral status and insurance/RPA recovery been prepared?
- Has the board of trustees, or delegated urgent reporting route, approved notification or been informed as soon as practicable?
- Has the fraud register been updated and has the Audit and Risk Committee been notified?

Document Detail	
Document Name:	Counter Fraud, Irregularity and Cybercrime Policy
Version:	1
Chief Officer Signature:	Signature
Effective From:	01/09/26
Approved by:	Approver Name
Approval Meeting Reference:	14/07/26
Next Review Date:	14/07/29

Version Control			
Version	**Date**	**Author**	**Change/Reference**
1	09/06/26	Claire Love (CFO)	Re-write
2	01/01/2024	Name	
3	01/01/2024	Name	